目次

概要

このドキュメントでは、Cisco IOS® ヘッドエンドで Lightweight Directory Access Protocol（LDAP）の認証を使用して、デフォルトの相対識別名（RDN）を Common Name（CN）から sAMAccountName に変更する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS ソフトウェア リリース 15.0 以降を実行する Cisco IOS デバイスに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

主な問題

LDAP ユーザがいるほとんどの Microsoft Active Directory（AD）では一般的に RDN を sAMAccountName として定義します。 VPN クライアントのヘッドエンドとして認証プロキシ（auth-proxy）および適応型セキュリティ アプライアンス（ASA）サーバを使用する場合は、AAA サーバを定義するときに AD サーバ タイプを定義するか、ldap-naming-attribute コマンドを入力するのであれば、簡単に修正されます。 ただし、Cisco IOS ソフトウェアでは、このいずれのオプションも使用できません。 デフォルトで、Cisco IOS ソフトウェアでは、ユーザ名の認証に AD の CN 属性値を使用します。 たとえば、AD でユーザ *John Fernandes* が作成されますが、ユーザ ID は *jfern* として保存されます。 デフォルトでは、Cisco IOS ソフトウェアは、CN 値をチェックします。 つまり、Cisco IOS ソフトウェアでは、ユーザ名の認証で *John Fernandes* をチェックし、sAMAccountName 値に *jfern* を認証でチェックしません。 Cisco IOS ソフトウェアで sAMAccountName の属性値からのユーザ名をチェックするように強制するには、このドキュメントで詳述されているダイナミック属性マップを使用します。

解決策

Cisco IOS デバイスでは RDN 変更の次の方法をサポートしていませんが、ダイナミックな属性マップを使用して Cisco IOS ソフトウェアで同様な結果を実現できます。 Cisco IOS ヘッドエンドで **show ldap attribute** コマンドを入力すると、次の出力が表示されます。

LDAP 属性	**書式**	**AAA 属性**
airespaceBwDataBurstContract	Ulong	bsn- data-bandwidth-burst-contr
userPassword	String	password
airespaceBwRealBurstContract	Ulong	bsn-realtime-bandwidth-burst-c
employeeType	String	employee-type
airespaceServiceType	Ulong	service-type
airespaceACLName	String	bsn-acl-name
priv-lvl	Ulong	priv-lvl
memberOf	String DN	supplicant-group
cn	**String**	**username**
airespaceDSCP	Ulong	bsn-dscp
policyTag	String	tag-name

airespaceQOSLevel	Ulong	bsn-qos-level
airespace8021PType	Ulong	bsn-8021p-type
airespaceBwRealAveContract	Ulong	bsn-realtime-bandwidth-average
airespaceVlanInterfaceName	String	bsn-vlan-interface-name
airespaceVapId	Ulong	bsn-wlan-id
airespaceBwDataAveContract	Ulong	bsn-data-bandwidth-average-con
sAMAccountName	String	sam-account-name
meetingContactInfo	String	contact-info
telephoneNumber	String	telephone-number

強調表示された属性からわかるように、Cisco IOS ネットワーク アクセス デバイス（NAD）では、認証の要求と応答に、この属性マップを使用します。 基本的に、Cisco IOS デバイスのダイナミック LDAP 属性マップは双方向で機能します。 つまり、属性は、応答を受信するときだけでなく、LDAP 要求が送信されるときにもマップされます。 ユーザ定義の属性マップである NAD 上の基本 LDAP 設定がない場合は、要求が送信されるときに次のログ メッセージが表示されます。

この動作を変更し、ユーザ名の確認に sAMAccountName の属性を使用するように強制する場合は、**ldap attribute map username** コマンドを入力して、このダイナミック属性マップをまず作成します。

```
ldap attribute map username   map type sAMAccountName username
```

この属性マップを定義したら、attribute map <dynamic-attribute-map-name> コマンドを入力して、選択した AAA サーバ グループ（aaa-server）にこの属性をマップします。

注このプロセス全体を簡単にするために、Cisco Bug ID CSCtr45874（登録ユーザ専用）がファイリングされました。 この機能要求が実装されていると、使用されている LDAP サーバをユーザが識別でき、その特定のサーバによって使用された値を反映するようにこれらのデフォルト マップの一部を自動的に変更できます。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定例

このドキュメントでは、次の設定を使用します。

- ダイナミック属性マップを定義するには、次のコマンドを入力します。**ldap attribute map** <dynamic-attribute-map-name> **map type sAMAccountName username**
- AAA サーバ グループを定義するには、次のコマンドを入力します。**aaa group server ldap** <server-group-name> **server** <server-name>
- サーバを定義するには、次のコマンドを入力します。**ldap server** <server-name> **ipv4** <host-address> **attribute map** <dynamic-attribute-map-name> **bind authentication root-dn** <complete-dn-root-user> **password** <root-user-pwd> **base-dn** <complete-dn-search-base>
- 使用する認証方式のリストを定義するには、次のコマンドを入力します。**aaa authentication login** <name> **group** <server-group-name>

AD ツール

ユーザの絶対識別名（DN）をチェックするには、AD のコマンド プロンプトから次のいずれかのコマンドを入力します。

dsquery user -name user1
または

dsquery user -samid user1
注上記の「user1」は regex 文字列です。 regex 文字列に「user*」を使用して、user から開始されるユーザ名を持つすべての DN を登録することもできます。

シングル ユーザのすべての属性を登録するには、AD のコマンド プロンプトで次のコマンドを入力します。

dsquery * -filter "(&(objectCategory=Person)(sAMAccountName=username))" -attr *

潜在的な問題

LDAP 導入では、検索操作が最初に実行され、バインド操作が後で実行されます。 この操作が実行されるのは、検索操作の一部としてパスワード属性が返される場合に、LDAP クライアントでローカル的にパスワード検証を実施でき、追加のバインド操作が不要であるためです。 パスワード属性が返されない場合は、バインド操作を後で実行できます。 検索操作を先に実行し、バインド操作を後で実行するもう一つの利点は、ユーザ名（CN 値）の前にベース DN が付加されているときに DN を形成するのではなく、検索結果で受け取った DN をユーザ DN として使用できる点です。

ユーザ名属性のマッピングのポイントを変更するユーザ定義属性とともに **authentication bind-first** コマンドを使用すると問題がある可能性があります。 たとえば、この設定を使用すると、認証を試行したときに通常は失敗します。

dsquery * -filter "(&(objectCategory=Person)(sAMAccountName=username))" -attr *
その結果、Invalid credentials, Result code =49 のエラー メッセージが表示されます。 次のようなログ メッセージが出力されます。

```
Oct  4 13:03:08.503: LDAP: LDAP: Queuing AAA request 0 for processingOct  4 13:03:08.503: LDAP:
Received queue event, new AAA requestOct  4 13:03:08.503: LDAP: LDAP authentication requestOct
4 13:03:08.503: LDAP: Attempting first  next available LDAP serverOct  4 13:03:08.503: LDAP: Got
next LDAP server :ss-ldapOct  4 13:03:08.503: LDAP: First Task: Send bind reqOct  4
13:03:08.503: LDAP: Authentication policy: bind-firstOct  4 13:03:08.503: LDAP: Dynamic map
configuredOct  4 13:03:08.503: LDAP: Dynamic map found for aaa type=usernameOct  4 13:03:08.503:
LDAP: Bind: User-DN=sAMAccountName=abcd,DC=qwrt,DC=comldap_req_encodeDoing socket writeOct  4
13:03:08.503: LDAP:  LDAP bind request sent successfully (reqid=36)Oct  4 13:03:08.503: LDAP:
Sent the LDAP request to serverOct  4 13:03:08.951: LDAP: Received socket eventOct  4
13:03:08.951: LDAP: Checking the conn statusOct  4 13:03:08.951: LDAP: Socket read event
socket=0Oct  4 13:03:08.951: LDAP: Found socket ctxOct  4 13:03:08.951: LDAP: Receive event:
```

```
read=1, errno=9 (Bad file number)Oct  4 13:03:08.951: LDAP: Passing the client
ctx=314BA6ECldap_resultwait4msg (timeout 0 sec, 1 usec)ldap_select_fd_wait
(select)ldap_read_activity lc 0x296EA104Doing socket readLDAP-TCP:Bytes read =
109ldap_match_request succeeded for msgid 36 h 0changing lr 0x300519E0 to COMPLETE as no
continuationsremoving request 0x300519E0 from list as lm 0x296C5170 all
0ldap_msgfreeldap_msgfreeOct  4 13:03:08.951: LDAP:LDAP Messages to be processed: 1Oct  4
13:03:08.951: LDAP: LDAP Message type: 97Oct  4 13:03:08.951: LDAP: Got ldap transaction context
from reqid    36ldap_parse_resultOct  4 13:03:08.951: LDAP: resultCode:    49     (Invalid
credentials)Oct  4 13:03:08.951: LDAP: Received Bind Responseldap_parse_result
ldap_err2string
```
Oct 4 13:03:08.951: LDAP: Ldap Result Msg: FAILED:Invalid credentials,   Result code =49Oct 4 13:03:08.951: LDAP: LDAP Bind operation result : failed
```
Oct  4 13:03:08.951: LDAP:
Restoring root bind status of the connectionOct  4 13:03:08.951: LDAP: Performing Root-Dn bind
operationldap_req_encodeDoing socket writeOct  4 13:03:08.951: LDAP: Root Bind on
CN=abcd,DC=qwrt,DC=cominitiated.ldap_msgfreeOct  4 13:03:08.951: LDAP: Closing transaction and
reporting error to AAAOct  4 13:03:08.951: LDAP: Transaction context removed from list [ldap
reqid=36]Oct  4 13:03:08.951: LDAP: Notifying AAA: REQUEST FAILEDOct  4 13:03:08.951: LDAP:
Received socket eventOct  4 13:03:09.491: LDAP: Received socket eventOct  4 13:03:09.491: LDAP:
Checking the conn statusOct  4 13:03:09.491: LDAP: Socket read event socket=0Oct  4
13:03:09.491: LDAP: Found socket ctxOct  4 13:03:09.495: LDAP: Receive event: read=1, errno=9
(Bad file number)Oct  4 13:03:09.495: LDAP: Passing the client ctx=314BA6ECldap_resultwait4msg
(timeout 0 sec, 1 usec)ldap_select_fd_wait (select)ldap_read_activity lc 0x296EA104Doing socket
readLDAP-TCP:Bytes read= 22ldap_match_request succeeded for msgid 37 h 0changing lr 0x300519E0
to COMPLETE as no continuationsremoving request 0x300519E0 from list as lm 0x296C5170 all
0ldap_msgfreeldap_msgfreeOct  4 13:03:09.495: LDAP: LDAP Messages to be processed: 1Oct  4
13:03:09.495: LDAP: LDAP Message type: 97Oct  4 13:03:09.495: LDAP: Got ldap transaction context
from reqid    37ldap_parse_resultOct  4 13:03:09.495: LDAP: resultCode:    0     (Success)P:
Received Bind    ResponseOct  4 13:03:09.495: LDAP: Received Root Bind Response
ldap_parse_resultOct  4 13:03:09.495: LDAP: Ldap Result Msg: SUCCESS, Result code =0Oct  4
13:03:09.495: LDAP: Root DN bind Successful on:CN=abcd,DC=qwrt,DC=comOct  4 13:03:09.495: LDAP:
Transaction context removed from list [ldap reqid=37]ldap_msgfreeldap_resultwait4msg (timeout 0
sec, 1 usec)ldap_select_fd_wait (select)ldap_err2stringOct  4 13:03:09.495: LDAP: Finished
processing ldap msg, Result:SuccessOct  4 13:03:09.495: LDAP: Received socket event
```

強調表示された行は、認証の前に最初のバインドで問題のある箇所を示します。 上記の設定から **authentication bind-first** コマンドを除去すると正常に動作します。

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show ldap attributes**
- **show ldap server all**

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

- debug ldap all
- debug ldap event
- debug aaa authentication
- debug aaa authorization

関連情報

- AAA LDAP 設定ガイド、Cisco IOS Release 15.1MT
- ASA 8.0： WebVPN ユーザのための LDAP 認証の設定
- テクニカルサポートとドキュメント - Cisco Systems